VTC Firewall Configuration

Purpose

A participating site may choose to connect the AVPN router to their existing firewall in order to support an existing VTC endpoint, or to provide versatility in placement of the CalEMA supplied VTC endpoint. This document describes the requirements for a firewall implementation. Communications regarding the installation of the VTC network should be directed to vtc-install@calema.ca.gov. Documentation for the CalEMA VTC project can be found at www.calema.ca.gov/vtc.

VTC Firewall Connection

The VTC interface of the AVPN router will either be connected directly to the firewall interface designated by the participating organization, or indirectly through the existing LAN infrastructure. The participating organization will be responsible for configuring any existing equipment required to connect the AVPN router into the site infrastructure. The connectivity of the associated equipment is depicted in the drawing titled "VTC Remote Detail"

In order to ensure that no conflicts arise between the CalEMA VTC network and the participating remotes, a subnet of six usable IP addresses has been assigned to each location from CalEMA's public address space. Requests for additional addressing will be reviewed by CalEMA. The AVPN router will use the lowest numbered address in the subnet, leaving five addresses to be assigned to VTC endpoints at the site. Address assignments from this subnet are static, and are configured directly on the VTC endpoint, except in the case of a firewall implementation. The firewall implementation uses Network Address Translation (NAT) to deliver IP packets to a VTC endpoint behind the firewall. One of the available public IP addresses are mapped to a static private IP address, configured on the VTC endpoint. A table of protocols and ports required for firewall traversal are included in this document. The CalEMA supplied VTC endpoints will be managed by CalEMA and require those protocols and ports in Table 1, while a VTC endpoint managed by the participating organization will require those in Table 2, at a minimum. Although the IP addresses being assigned are publicly routable, the AVPN network does not traverse the Internet, nor does it provide access to the Internet. The participating site will require a static route to the VTC networks (204.235.52.0 /22, 204.235.56.0 /22), pointed to the VTC interface of the AVPN router.

VTC Endpoints

Registration of the VTC endpoints with CalEMA is required for proper operation. The registration of a VTC endpoint is performed by completing the document titled "VTC Endpoint Registration," and sending it to vtc-register@calema.ca.gov. The registration process ensures organized expansion of the OASIS five digit dial plan to include the VTC endpoints, as well as identifying the allocated IP addresses within the VTC network.

CalEMA has selected Tandberg as the manufacturer of the VTC endpoints being deployed to the participating sites. The deployment of a standard equipment configuration enables CalEMA to effectively manage the endpoints. CalEMA supports the use of VTC equipment not provided by CalEMA in the VTC network, but is subject to some restrictions. Interoperability issues may exist, depending on the manufacturer and model.

VTC Firewall Protocol and Port Utilization

Table 1 – CalEMA Managed VTC Endpoint

Source	Destination	Protocol	Port	Service	Purpose
204.235.55.0/24, 204.235.56.0/24	<VTC Endpoint>	TCP	21	FTP/Control	Management
204.235.55.0/24, 204.235.56.0/24	<VTC Endpoint>	TCP	23	Telnet	Management
204.235.55.0/24, 204.235.56.0/24	<VTC Endpoint>	TCP	80	Http	Management
204.235.55.0/24, 204.235.56.0/24	<VTC Endpoint>	UDP	161	SNMP/queries	Management
<VTC Endpoint>	204.235.55.0/24, 204.235.56.0/24	UDP	162	SNMP/traps	Management
204.235.55.0/24, 204.235.56.0/24	<VTC Endpoint>	TCP	443	Https	Management
<VTC Endpoint>	204.235.55.0/24, 204.235.56.0/24	TCP	963	Netlog	Management
204.235.55.0/24, 204.235.56.0/24	<VTC Endpoint>	TCP	1026	FTP/data	Management
<VTC Endpoint>	204.235.55.0/24, 204.235.56.0/24	UDP	123	NTP	Operations
204.235.52.0/22, 204.235.56.0/22	<VTC Endpoint>	TCP	1720	H.323/Q931	Operations
204.235.52.0/22, 204.235.56.0/22	<VTC Endpoint>	UDP	1719	H.323/RTP	Operations
204.235.52.0/22, 204.235.56.0/22	<VTC Endpoint>	TCP	1503	H.323/H.245	Operations

Table 2 – Non-managed VTC Endpoint

Source	Destination	Protocol	Port	Service	Purpose
<VTC Endpoint>	204.235.55.0/24, 204.235.56.0/24	UDP	123	NTP	Operations
204.235.52.0/22, 204.235.56.0/22	<VTC Endpoint>	TCP	1720	H.323/Q931	Operations
204.235.52.0/22, 204.235.56.0/22	<VTC Endpoint>	UDP	1719	H.323/RTP	Operations
204.235.52.0/22, 204.235.56.0/22	<VTC Endpoint>	TCP	1503	H.323/H.245	Operations